UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/737,109	12/15/2003	Jianxin Wang	063170.6722	5512

5073 7590 01/02/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
LE, MIRANDA	
ART UNIT	**PAPER NUMBER**
2169	

NOTIFICATION DATE	DELIVERY MODE
01/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/737,109	WANG, JIANXIN	
	Examiner	Art Unit	
	MIRANDA LE	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/24/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/15/08 has been entered.

This communication is responsive to Amendment, filed 10/15/08.

Claims 1-34 are pending in this application. Claims 1, 13, 25, 34 are independent claims. Claims 1, 13, 25 have been amended. This action is made non-Final.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless:
>
> (e) the invention was described in
>
> (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or
>
> (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application

designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 34 is rejected under 35 U.S.C. 102(e) as being anticipated by Spilo et al. (US Patent No. 6,208,999).

Spilo anticipated independent claim 34 by the following:

As per claim 34, Spilo teaches a serverless backup method comprising:

opening a file system root directory *(i.e. The file system of the invention includes file identification information with file data, thereby enhancing prospects for file recovery in the event of file system damage. Moreover, the entire directory structure for the storage device, including all subdirectories, is maintained in a single data structure. If this data structure is damaged, it can be completely recreated from information recovered from other areas of the storage device, col. 4, lines 38-46)*;

parsing the file system root directory for allocation tables of each file and finding attributes of each file *(Each directory entry within the directory structure contains the entire pathname to a data file. Accordingly, a hierarchical structure, such as a FAT system, is simulated by the invention. In a preferred embodiment, the invention is compatible with and is used in conjunction with a hierarchical file system, such as FAT or NTFS, col. 4, line 56-65)*;

examining the attributes of each file and determining whether a file is resident or non resident *(i.e. the disk can be scanned to find missing files, col. 4, line 66 to col. 5, line 11; a flag in the directory entry and in each data block is set to indicate that the file is no longer present, col. 10, lines 12-16)*;

backing up entire attributes of a file *(i.e. A second possible mode of operation is to back up files asynchronously (e.g. during idle time or at prespecified intervals). Again, a supervisory program monitors disk operations, tracking those files that have been created or changed on the FAT file system. Then, periodically or during idle time, the supervisory program takes appropriate action to copy, modify, or erase the data on the device embodying the file system, as indicated by the tracking information discussed above, col. 10, lines 57-65)* if it is determined that the file is resident *(i.e. File allocation information can be dynamically maintained and can be reconstructed in cases of loss or damage by scanning the disk for blocks having identification and sequence numbers, col. 4, line 66 to col. 5, line 11)*; and

backing up attributes and data blocks belonging to the file *(i.e. A second possible mode of operation is to back up files asynchronously (e.g. during idle time or at prespecified intervals). Again, a supervisory program monitors disk operations, tracking those files that have been created or changed on the FAT file system. Then, periodically or during idle time, the supervisory program takes appropriate action to copy, modify, or erase the data on the device embodying the file system, as indicated by the tracking information discussed above, col. 10, lines 57-65)* if it is determined the file is not resident *(i.e. Only a small portion of each data file block is devoted to the information used to recreate the file and directory structures, col. 5, lines 12-25)*.

Claims 1-5, 13-17, 25-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Dunham et al. (US Patent No. 6,269,431).

Dunham anticipated independent claims 1, 13, 25 by the following:

As per claim 1, Dunham teaches a serverless backup system for backing up information on a network including one or more servers, comprising

a storage system *(See Figs. 1, 2)* for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to:

receive the information *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)* from a plurality of workstations *(i.e. Host 31, 32, 33, Fig. 2)*; and

store the information *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data*

storage subsystem 22, col. 5, lines 14-25) received from the plurality of workstations *(i.e. The hosts 31, 32, 33, for example, are workstations of respective users 34, 35, 36, col. 8, lines 16-43)*; and

a backup storage system for backing up the information *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the backup storage system coupled to the storage system and to one or more servers via network *(i.e. Control station server 76, 77, See Fig. 4)*;

wherein:

the information being backup is transferred using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being backed up directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system *(i.e. primary data storage, col. 1, line 60 to col. 2, line 18)* to the backup storage system *(i.e. the backup versions are stored in secondary data storage, col. 1, line 60 to col. 2, line 18)* without going through the one or more servers *(i.e. specified data in the primary storage 27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44)*; and

the information being restored is transferred using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system *(i.e. the backup versions are stored in secondary data storage, col. 1, line 60 to col. 2, line 18)* to the storage system *(i.e. primary data storage, col. 1, line 60 to col. 2, line 18)* without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*.

As per claim 13, Dunham teaches a serverless backup method for backing up information on a network including one or more servers, comprising:

providing a storage system *(See Figs. 1, 2)* for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to:

receive the information from a plurality of workstation *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*; and

store the information received from the plurality of workstations *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*;

providing a backup storage system for backing up the information *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the backup storage system coupled to the storage system and to one or more servers via a network *(i.e. Control station server 76, 77, See Fig. 4)*;

backing up the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to

transfer the information being backed up directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system to the backup storage system without going through the one or more servers *(i.e. specified data in the primary storage 27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44)*; and

restoring information by transferring information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system to the storage system without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*.

As per claim 25, Dunham teaches a computer readable medium including code for performing a serverless backup method for backing up information on a

network, the network including a storage device for storing information to be backed up and restored *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*, the storage system operable to receive the information form a plurality of workstations and store the information received from the plurality of workstations *(i.e. The host computer 20 is operated by a user 23, and during typical operation the host computer reads and writes to primary storage 27 in the primary data storage subsystem 21. In order to recover from a failure causing a loss of data in the primary storage 27, a backup copy of data in the primary storage 27 is kept in secondary storage 29 of the secondary data storage subsystem 22, col. 5, lines 14-25)*, the network further including a backup storage system for backing up the information, the backup storage system coupled to the storage system and to one or more servers via the network, the code comprising:

code for backing up the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being backed up directly*(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the storage system to the backup storage system without going through the one or more servers *(i.e. specified data in the primary storage*

27 is copied to the secondary storage 29 when the primary data storage subsystem 21 receives a backup command from the host 20, col. 5, lines 26-44); and

code for restoring the information by transferring the information using one or more data movers *(i.e. data mover 72, 73, 74, 75, See Fig. 4)* operable to transfer the information being restored directly *(i.e. The storage controller has at least one data port for linking the primary data storage and the secondary data storage to the host processor for transfer of data between the primary data storage and the secondary data storage and the host processor, col. 3, line 48 to col. 4, line 23)* from the backup storage system to the storage system without going through the one or more servers *(i.e. The data storage subsystem has primary data storage, and the backup versions are stored in secondary data storage linked to the data storage subsystem for transfer of the backup versions from the secondary data storage to the data storage subsystem, col. 1, line 60 to col. 2, line 18)*.

As to claims 2, 14, Tamura teaches the system as recited in Claim 1, wherein the backup storage system comprises a tape storage system *(i.e. a tape or DLT library, col. 2, lines 10-25)*.

As to claims 3, 15, Tamura teaches the system as recited in Claim 1, wherein the storage system comprises a disk storage system *(i.e. The present invention provides a method, a system and code for backing up information on a*

storage system, for example, a disk system, connected to a storage area network, col. 2, lines 10-25).

As to claims 4, 16, Tamura teaches the system as recited in Claim 1, wherein the backup storage system comprises a storage area network *(i.e. The storage system is coupled with the plurality of backup systems via a storage area network (SAN). The method includes the storage system receiving a command to copy the information, from the server. Next, the storage system finds an available backup system; and under control of the storage system, the information is copied to the available backup system, col. 2, lines 25-35)*.

As to claims 5, 17, 26, Tamura teaches the system as recited in Claim 1, wherein the information is transferred between the backup storage system and the storage system using Extended Copy command *(i.e. The present invention provides a method, a system and code for backing up information on a storage system, for example, a disk system, connected to a storage area network. The host or server system off loads the task of backing up its data to the storage system that stores the data. In an exemplary embodiment a server sends an E-Copy command to a copy manager on a disk system. Next, the copy manager finds an available back-device, for example a tape or DLT library, and then backups the information indicated in the E-Copy command to the back-up device. A user interface is provided so that one or more path groups, comprising at least*

a target port and an initiator port, on a disk system may be designated, col. 2, lines 10-25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 6, 7, 18, 19, 27, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamura (US Patent No. 6,728,848), in view of West et al. (US Patent No. 6,446,175).

As to claim 6, 18, 27, Tamura does not specifically prior to transferring information directly from the storage system to the backup storage system, a snapshot of the storage system is taken.

West teaches this limitation *(i.e. as shown in FIG. 5, a snap volume 154 is used to reduce the impact on the remote host system 128. That is, snap volume 154 is used as temporary or bridge volume, established in the manner described above with respect to FIG. 1, so the host 128 may access the secondary temporary volumes 150 as necessary. The snap processes for snap volumes 154 is represented by arrows 158 and bit map structures 160 and 162 can be used to facilitate partial volume restoration or snapping procedures based on bit map information. Moreover, a primary temporary volume 156 may be established to receive the point-in-time copy information as shown in FIG. 5. The data transfer is handled in the same manner as the data transfers from the primary to the secondary during normal backup, however, the data is transmitted in the opposite direction using link 119 to the temporary volume 156. The secondary system 104 is the transmitting system and the primary system 102 is the receiving system. Each controller 110 and 116 is configured to both send and receive data information along links 118 and 119, col. 15, lines 10-30)*.

It would have been obvious to one of ordinary skill of the art having the teaching of Tamura and West at the time the invention was made to modify the system of Tamura to include the limitations as taught by West. One of ordinary skill in the art would be motivated to make this combination in order to receive the point-in-time copy information in view of West (col. 15, lines 10-30), as doing

so would give the added benefit of reducing the impact on the remote host system as taught by West (col. 15, lines 10-30).

As to claims 7, 19, 28, Tamura teaches a period of write inactivity to the storage system is waited *(i.e. waits for the next bitmap table to be placed in the shared memory by another target JOB, col. 9, lines 6-55)*.

West teaches taking the snapshot *(i.e. as shown in FIG. 5, a snap volume 154 is used to reduce the impact on the remote host system 128. That is, snap volume 154 is used as temporary or bridge volume, established in the manner described above with respect to FIG. 1, so the host 128 may access the secondary temporary volumes 150 as necessary. The snap processes for snap volumes 154 is represented by arrows 158 and bit map structures 160 and 162 can be used to facilitate partial volume restoration or snapping procedures based on bit map information, col. 15, lines 10-30)*.

Claims 8, 9, 20, 21, 29, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamura (US Patent No. 6,728,848), in view of West et al. (US Patent No. 6,446,175), and further in view of Gold et al. (US Patent No. 6,785,786).

As to claims 8, 20, 29, Tamura, West do not specifically teach the period of write inactivity is a predefined period of time.

Gold teaches this limitation *(i.e. if the time is set to 5 seconds, col. 5, lines 55-67*).

It would have been obvious to one of ordinary skill of the art having the teaching of Tamura, West, and Gold at the time the invention was made to modify the system of Tamura, West to include the limitations as taught by Gold. One of ordinary skill in the art would be motivated to make this combination in order to determine when a file is safe to backup in view of Gold (col. 5, lines 54-67), as doing so would give the added benefit of a data restore operation can be enacted using data stored in primary storage, without needing to find and install any particular backup tape (col. 2, lines 9-14) as taught by Gold.

As to claims 9, 21, 30, Tamura, West, Gold do not teach the system as recited in claim 8, wherein the predefined period of time is three seconds.

However, Gold teaches "*if the time is set to 5 seconds" (col. 5, lines 54-67)*.

It would have been obvious to one ordinary skill of the art having the teaching of Tamura, West, and Gold at the time the invention was made to set the predefined period of time of Gold to three seconds in order to determine when a file is safe to backup as taught by Gold (col. 5, lines 55-67), as doing so would give the added benefit of a data restore operation can be enacted using data stored in primary storage, without needing to find and install any particular backup tape (col. 2, lines 9-14) as taught by Gold.

Claims 10-12, 22-24, 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamura (US Patent No. 6,728,848), in view of West et al. (US Patent No. 6,446,175), and further in view of Blam et al. (US Patent No. 6,738,923.

As to claims 10, 22, 31, Tamura, West do not specifically teach if the period of write inactivity does not occur by time a timeout period has expired, the transfer fails.

Blam teaches a timeout period *(col. 4, line 65 to col. 5, line 27)*.

It would have been obvious to one of ordinary skill of the art having the teaching of Tamura, West, and Blam at the time the invention was made to modify the system of Tamura, West to include the limitations as taught by Blam. One of ordinary skill in the art would be motivated to make this combination in order to access and boot from the next backup server in the network (col. 5, lines 15-27) in view of Blam, as doing so would give the added benefit of a method for adjusting time-outs and failover intervals according to the requirements of different systems (col. 1, line 65 to col. 2, line 3) as taught by Blam.

As to claims 11, 23, 32, Blam teaches timeout period is a predefined period of time *(col. 4, line 65 to col. 5, line 27).*

As to claims 12, 24, 33, Tamura, West, Blam do not explicitly teach the predefined period of time is 80 seconds.

However, Blam teaches *"a method of adjusting failover intervals" (col. 5, lines 59-67).*

It would have been obvious to one ordinary skill of the art having the teaching of Tamura, West, Blam at the time the invention was made to use the method of Blame to adjust the predefined period of time is 80 seconds in order to access and boot from the next backup server in the network as taught by Blam (col. 5, lines 15-27), as doing so would give the added benefit of a method for adjusting time-outs and failover intervals according to the requirements of different systems (col. 1, line 65 to col. 2, line 3) as taught by Blam.

Response to Arguments

Applicant's arguments filed 10/15/08 have been fully considered but they are not persuasive.

1. Claims 1, 13, 25

Applicant's arguments with respect to claims 1, 13, 25 have been considered but are moot in view of the new ground(s) of rejection.

2. Determining whether a file is resident or non-resident (Claim 34)

Spilo reads on claim 34 as follows:

The file is resident equates to system files and documents of Spilo, col. 10, lines 42-56 *(i.e. The supervisory program can be enabled to distinguish between critical data (e.g. system files and documents) and non-critical data (e.g. temporary files and other easily recreatable files) so that only the critical files are*

backed up; this can significantly decrease the space overhead required by the invention, col. 10, lines 42-56).

The file is resident also equates to the file identification numbers 1-100, or system files of Spilo, col. 8, lines 3-18 *(i.e. The file identification and file sequence numbers can be implemented as follows. Every file is assigned a unique file identification number, based on its location within the directory structure discussed above. If there are 100 files using the file system, then file identification numbers 1-100 can be used, col. 8, lines 3-18)*.

The file is non-resident equates to temporary file of Spilo, col. 10, lines 42-56 *(i.e. The supervisory program can be enabled to distinguish between critical data (e.g. system files and documents) and non-critical data (e.g. temporary files and other easily recreatable files) so that only the critical files are backed up; this can significantly decrease the space overhead required by the invention, col. 10, lines 42-56)*.

The file is non-resident further equates to the file identification number is not related to a file's position within the directory structure of Spilo, col. 8, lines 3-18.

3. Backing up entire attributes of a file if it is determined that the file is resident (Claim 34)

Backing up entire attributes equates to only the critical files are backed up of Spilo, col. 10, lines 42-56 (*i.e. The supervisory program can be enabled to*

distinguish between critical data (e.g. system files and documents) and non-critical data (e.g. temporary files and other easily recreatable files) so that only the critical files are backed up; this can significantly decrease the space overhead required by the invention, col. 10, lines 42-56).

Backing up entire attributes also equates to writing the tracking information to each block of the critical files of Spilo, col. 10, line 66 to col. 11, line 12 *(i.e. The application program, when writing certain data files deemed to be critical, writes the tracking information (e.g. the file identification number 62, the sequence number 64, and the unique bit pattern 66) to each block of the critical files, col. 10, line 66 to col. 11, line 12).*

4. Backing up attributes and data blocks belonging to the file if it is determined that the file is non-resident (Claim 34)

Backing up attributes and data blocks equates to the file identification number should be stored within the file's directory entry, col. 8, lines 3-18 *(i.e. If the file identification number is not related to a file's position within the directory structure, then the file identification number should be stored within the file's directory entry, as discussed above, col. 8, lines 3-18).*

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Miranda Le whose telephone number is (571) 272-4112. The examiner can normally be reached on Monday through Friday from 10:00 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James K. Trujillo, can be reached at (571) 272-3677. The fax number to this Art Unit is (571)-273-8300.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Miranda Le/
Primary Examiner, Art Unit 2169